

**EXHIBIT D**

**Tax Compliance SOW**



## STATEMENT OF WORK

This Statement of Work ("SOW") dated March 29, 2024 is governed by and subject to the provisions of the agreement dated July 11, 2012, as reinstated and amended (the "Agreement"), the terms of which are incorporated herein, between Big Lots Stores, LLC (formerly Big Lots Stores, Inc.) and the PwC US firm named therein. The term "Client" or "you" in the Agreement shall include the entity(ies) signing this SOW. For purposes of this SOW, the terms "we", "us" or "PwC" in the Agreement and this SOW mean PwC US Tax LLP. Client's consolidated subsidiaries and affiliates are bound to the terms of the Agreement and this SOW to the extent Client procures services under this SOW on their behalf. Any terms used in this SOW and not otherwise defined will have the same meaning as in the Agreement. If there is a conflict between the Agreement and the SOW, this SOW shall prevail.

### I. PURPOSE AND SCOPE

This SOW sets forth the objectives, deliverables, timing, staffing and fees for this project/effort.

### II. PARTIES' RESPONSIBILITIES

#### **2.1 Services to be provided by PwC:**

This SOW covers the following services (the "Services"):

##### (a) 2023 Tax Compliance Services

PwC will provide assistance in the preparation of the U.S. federal income tax return for Client for the tax year beginning January 29, 2023 through February 3, 2024, as requested by Client, as outlined in Exhibit I. Client and PwC agree that PwC is a non-signing preparer for purposes of Client's federal income tax return and that Deloitte & Touche LLP ("Deloitte") will review and sign the federal return as paid preparer.

PwC will prepare and sign as preparer the U.S. state and local tax returns for Client for the tax year beginning January 29, 2023 through February 3, 2024, as requested by Client for itself and certain entities, as listed in Exhibit I. Client and PwC may mutually agree in writing (including e-mail) to revise the listing of entities and tax returns included in Exhibit I and make a related adjustment to our fees. Entities listed in Exhibit I are considered Affiliates and are also bound to the terms of this SOW. Specific detail, responsibilities, and scope regarding the nature of exact deliverables agreed to and or impacting the Services are also included in Exhibit I.

We will complete Schedule UTP, if applicable, based on information you provide to us during the course of the engagement. We may gather such information by providing you with a checklist or information request during the course of the engagement. To the extent you require additional assistance to gather and analyze information for purposes of the Schedule UTP reporting, such services will be the subject of a separate SOW.

Unless otherwise agreed with PwC, Client will be responsible for preparation and filing of all other required tax or information returns, including, for example, city and county income or gross receipts filings, payroll tax filings, sales and use tax filings, information reporting filings, etc.



Big Lots Stores, LLC  
March 29, 2024

Client is required to maintain and retain adequate documentation to support the tax returns as filed, as penalties can be imposed by taxing authorities for the failure to produce adequate documentation supporting items included in a tax return.

Client is responsible for understanding and agreeing with the amounts, computations, and statements made in all of the tax returns before they are filed with the taxing authorities. Most of the tax returns that PwC will prepare require the taxpayer to sign, under the penalties of perjury, affirming that the tax returns and the accompanying schedules and statements are true, correct, and complete to the best of his or her knowledge.

It is our understanding that you will file the returns as prepared by PwC unless you inform us otherwise. For those returns that PwC agrees to be the Electronic Return Originator (see Electronic Filing below), PwC will file those returns electronically after you have reviewed and approved the returns for filing.

Client is required to maintain and retain adequate documentation to support the tax returns as filed as penalties can be imposed by taxing authorities for the failure to produce adequate documentation supporting the items included in a tax return.

We will complete the preparation of the state income and franchise tax returns so they can be timely filed by the extended due date as agreed upon between PwC and Client. Client will have overall responsibility for filing the federal income tax return and all related statements and disclosures by the extended due date. In the event the agreed timetable requires that Client provide us with needed information or assistance within a specified period of time, the failure to timely provide this assistance may require adjustment to our completion date. In addition, in the event unforeseen circumstances occur that impact our ability to meet the final completion date, we will contact Client to discuss an acceptable revised completion date.

The rules for outbound transfers of stock (and certain asset transfers treated as indirect transfers of stock) under Internal Revenue Code Section 367(a) and associated regulations are complex. You are responsible for identifying transactions for which gain recognition agreements ("GRAs") are required to qualify for an exception from gain recognition under Internal Revenue Code Section 367, and if so, the adequacy of any disclosure. The Services set forth herein do not include preparing or reviewing such GRAs and related disclosures. To the extent that you subsequently request us to provide such additional services, the mutually agreed services and fees will be set forth in a Statement of Work.

The potential implications of proposed or recently enacted tax rules are complex and interpretative guidance for aspects of these rules may not be available. The Services set forth herein include basic consideration of the proposed or recently enacted rules and related reporting requirements but do not include performing every analysis that may need to be undertaken during this engagement to address these changes. To the extent that you request or we identify additional items related to assessing the impact associated with these rules and related reporting requirements, we will do so (a) pursuant to a separate written agreement, or (b) in accordance with the Additional Services provisions of our agreement with you, in either case based on mutually agreed Services and fees.

The Internal Revenue Service ("IRS") guidance addressing the taxation of virtual currency transactions provides that virtual currency (such as Bitcoin, Ether, etc.) is treated as property for



Big Lots Stores, LLC  
March 29, 2024

federal tax purposes. Therefore, general tax principles that apply to property transactions must be applied to exchanges of virtual currencies, which include cryptocurrencies and non-crypto virtual currencies. Generally, U.S. taxpayers must report all sales, exchanges, and other dispositions of any virtual currency. An exchange of a virtual currency includes the use of the virtual currency to pay for or purchase goods, services, or other property, including another virtual currency such as exchanging Bitcoin for Ether. This obligation applies regardless of whether the account is held in the U.S. or abroad. You must report virtual currency transactions on your return, regardless of whether you received a payee statement for the transaction (such as a Form W-2, Form 1099, etc.) or not. To the extent that you engaged in any virtual currency transactions during the year, please provide the details to us for consideration in connection with the preparation of your tax return. If you received a reporting virtual currency transactions letter from the IRS or another tax authority, please provide us with a copy of that letter. We will contact you if we believe additional work needs to be conducted related to your virtual currency transactions and the related fees, if any, for such additional work.

#### (b) Subsequent Year's Tax Compliance Services

For tax compliance and related planning purposes, it is common to provide services for the subsequent tax year as mutually agreed. Such services relating to recurring and non-recurring tax work such as the preparation of year end estimates, estimated tax payments, allocation, extensions, compliance coordination and related tax consulting will be covered under the terms and conditions of this SOW with mutually agreed upon adjustment for fees.

#### **2.2 Additional provisions applicable to the Services:**

In the event the agreement is terminated, this SOW shall remain in full force and effect in accordance with its terms, including the terms and conditions of the agreement, which are incorporated herein by reference.

The provisions of the Data Protection Exhibit hereto shall apply to the extent that PwC processes Client Personal Information (as that term is defined in the Data Protection Exhibit) in connection with its performance of Services hereunder. The Data Protection Exhibit attached to this SOW, supersedes and replaces any previous Data Protection Exhibit included in the Agreement, if any, solely for purposes of this SOW.

#### **Prospective Financial Information**

PwC may advise or assist Client in connection with its consideration, preparation or accumulation of prospective financial statements or other forward-looking information, including forecasts or projections (collectively, "PFI"), based on Client's instructions, using information, procedures and methods approved by Client. Client is responsible for the information used to prepare PFI, any decisions, assumptions or projections relating to PFI or any outputs therefrom and their adequacy for Client's purposes. Client shall ensure that any prospective financial statements or other information or materials prepared by PwC are reviewed and approved by the member of Client's management team responsible for the information, its accuracy, completeness, reasonableness and use. PwC may prepare ranges of quantitative estimates using PwC-identified illustrative assumptions of individual future costs or benefits for the purpose of illustrating PwC's advice; the estimates may be based on historical data, benchmarks, experience, the engagement team's knowledge of leading practices. PwC also may perform sensitivity, vulnerability or "what if" simulations or analyses on PFI and any underlying assumptions, or make recommendations on



Big Lots Stores, LLC  
March 29, 2024

assumptions not included in the PFI. PwC's observations and any quantified alternatives, sensitivities or vulnerabilities do not represent PwC's assurance, concurrence, conclusion or opinion on any PFI, nor PwC's advocacy, endorsement or promotion of any results therefrom and are not intended to be used by Client as its own PFI; they are only an illustration of PwC's advice to Client regarding Client's evaluation or determination of PFI. It is Client's responsibility to make its own decisions regarding PFI. As events and circumstances frequently do not occur as expected, there may be material differences between PFI and actual results; PwC disclaims any responsibility and liability for PFI, or based on any differences between PFI and any actual results achieved.

### **FinCEN Form 114 (Report of Foreign Bank and Financial Accounts)**

Federal law requires that certain individuals and entities report financial interests in, and signatory authority or certain other authority over, foreign financial accounts with more than \$10,000 in aggregate value in a calendar year on FinCEN Form 114, Report of Foreign Bank and Financial Accounts. This form is not filed with a tax return. Instead this form must be filed electronically with the U.S. Department of the Treasury through the Financial Crimes Enforcement Network's ("FinCEN's") BSA E-filing System by April 15 of the year following the calendar year in which aggregate amounts held in the foreign financial accounts meet the threshold. The definition of financial accounts is broadly defined and includes certain interests held indirectly. Failure to comply with these laws could result in significant civil and criminal penalties. Unless specifically listed on the Listing of Tax Returns to be Prepared, PwC will not prepare, file, or provide assistance with respect to the FinCEN Form 114.

### **IRS Form 8938**

Federal law requires that certain individuals and entities include in their income tax returns for any year, a report of all specified foreign financial assets held by them during that year. This reporting, on IRS Form 8938, is required when the taxpayer's specified foreign financial assets exceed a specific threshold during any year. The data gathering, valuation, and associated reporting is complex. Therefore, it is not included in the normal scope of tax services provided under this agreement, and our fee for performing these services will be billed separately based on the hourly rates specified below.

### **Electronic Filing**

The Internal Revenue Service and some states (collectively, "taxing authorities") offer or require electronic filing for certain tax returns. As part of the services covered by our agreement with you, PwC may be designated as the Electronic Return Originator ("ERO") for the tax filings we prepare under this agreement. Your designation of PwC as the ERO allows taxing authorities to disclose to us: (1) any acknowledgement that your tax filings(s) have been accepted by the taxing authority, (2) the reason(s) for any delay in processing a tax filing or refund, and (3) information regarding any refund offset. For those returns that PwC agrees to be the ERO, PwC will file those returns electronically after you have reviewed and approved the returns for filing. For all other returns, it is our understanding that you will file the returns as prepared by PwC unless you inform us otherwise. If a particular return is ineligible or unable to be processed electronically after making reasonable efforts to do so pursuant to the procedures established by the appropriate taxing authority, PwC will provide you with a paper return that must be filed by you in accordance with the terms noted in our agreement with you.



Big Lots Stores, LLC  
March 29, 2024

### **Use of PwC Technology**

Certain internet-based PwC Technology (as defined below) may be made available to you during our engagement as a convenience to support PwC's provision of Services to you. PwC Technology that may be provided to you include PwC's proprietary collaboration tools, software, databases, portals and platforms, all related documentation, as well as any modifications, derivatives or enhancements to them (collectively "PwC Technology"). Should you elect to use such PwC Technology, you understand that access to the PwC Technology is provided "as is" without any express or implied warranties. Upon PwC's request, Client must inform Client's PwC team of the names of the Client personnel whom the Client authorizes to access and use the PwC Technology on Client's behalf (the "Client Users"). Client will give access to the PwC Technology to only its employees and those third party consultants and contractors of Client who need access in order to provide services to Client and such employees and third parties are deemed "Client Users" for purposes of this SOW. If a Client User no longer needs access or if a Client User's access rights related to your information needs changes, you will notify PwC of same within a commercially reasonable period of time and PwC will make such access changes. You shall remain responsible for all use and access of the PwC Technology by Client Users. Any access credentials issued by PwC are unique to each Client User and must not be shared, even between Client Users.

The information available to you on or through the PwC Technology during an engagement shall be information relating to the performance and delivery of the relevant Services and Deliverables, and if applicable, information relating to the twelve (12) month period preceding such relevant Services and Deliverables. PwC Technology is not designed or intended to form part of your permanent records, and you are responsible for making and separately maintaining copies of any records stored on the PwC Technology that may be needed by you.

PwC Technology and all materials related to it (including the underlying technology, user interface, algorithm, process, functionality etc.), are confidential and proprietary to PwC. As between the parties, PwC is and shall remain the sole owner of all rights, title and interests therein and thereto (but excluding any information or other content you place in the PwC Technology). You (and any permitted Client Users) may only use the PwC Technology to access, share and view certain information in connection with your receipt of Services, and other than the foregoing permission, no express or implied right or license is granted. Your access to the PwC Technology shall end at the conclusion of the applicable Services. You shall not (and shall not allow any Client User to) misappropriate or infringe any of PwC's rights in PwC Technology, or otherwise do anything that you are not expressly permitted to do under this SOW, or which would interfere with PwC's rights to such PwC Technology. PwC reserves the right, at its discretion, to change or discontinue the offerings, content, information, functionality and availability of the PwC Technology consistent with the Security Controls (defined in the Data Protection Exhibit).

### **Reportable Transaction Disclosures and Listing Requirements**

Certain federal and state regulations require taxpayers to disclose their participation in certain reportable transactions to the taxing authorities. Client shall advise PwC if Client determines that any matter covered by this engagement letter is a reportable transaction that is required to be disclosed. Upon your request, we will provide a Reportable Transaction Compliance checklist to



Big Lots Stores, LLC  
March 29, 2024

assist you. PwC time spent preparing or reviewing Form(s) 8886 is outside the scope of this engagement letter and may be performed as mutually agreed with you.

Certain federal and state regulations also require PwC to submit information returns and maintain lists of certain client engagements if PwC is a material advisor to clients that have participated in a reportable transaction. Therefore, if PwC determines, after consultation with Client, that Client has participated in a transaction causing PwC to have a registration and/or list maintenance obligation, PwC will place Client's name and other required information on a list. PwC will contact Client if PwC is required to provide Client's name to the U.S. Internal Revenue Service or any state in connection with any matter under this SOW.

Certain laws and/or regulations, including those adopted because of the European Union Council Directive (EU) 2018/822 of May 25, 2018, amending Directive 2011/16/EU, require advisors or taxpayers to disclose certain transactions to a tax authority. These laws may require disclosure of certain transactions by PwC or by Other PwC Firms. The parties shall cooperate with each other to allow the filing of such disclosures. If PwC reasonably believes it is required to make such disclosure, PwC will make the disclosure, or where applicable, coordinate with Other PwC Firms, if disclosure is required by Other PwC Firms. Where PwC or Other PwC Firms are required to make such a disclosure, where practicable, PwC will share that disclosure with Client before it is filed.

### **2.3 Deliverables:**

Deliverables will be outlined in Exhibit I as requested by the Client. Client and PwC may mutually agree in writing (including email) to revise the listing of deliverables included in Exhibit I and make a related adjustment to our fees.

### **2.4 Our Responsibilities**

We will perform the Services in accordance with the Statements on Standards for Tax Services established by the American Institute of Certified Public Accountants. Accordingly, we will not provide an audit or attest opinion or other form of assurance, and we will not verify or audit any information provided to us.

We will complete the preparation of the tax returns based on a mutually agreed upon schedule so they can be timely filed by the extended due date as agreed upon between PwC and Client.

### **2.5 Client's Responsibilities:**

To facilitate PwC's work, Client will need to provide the following assistance:

- Any pertinent supporting documentation in relation to Client's 2023 income and deductions.
- Client is responsible for mailing the tax returns to the appropriate tax authorities.

We expect that you will provide timely, accurate and complete information and reasonable assistance, and we will perform the engagement on that basis.





Big Lots Stores, LLC  
March 29, 2024

You are responsible for all management functions and decisions relating to this engagement, including evaluating and accepting the adequacy of the scope of the Services in addressing your needs. You are also responsible for the results achieved from using any Services or deliverables, and it is your responsibility to establish and maintain your internal controls. You will designate a competent member of your management to oversee the Services.

#### **2.6 Timing:**

The timing of the Services is as follows:

Project Effective Date:	The earlier of the date PwC began services, or the signing of this SOW
Estimated Project Completion Date:	December 31, 2024

If we perform the Services prior to both parties executing this SOW, this SOW shall be effective as of the date we began the Services.

### **III. RESOURCES ASSIGNED**

The PwC personnel assigned to provide Services and deliverables under this SOW are as follows:

- Craig Keller, Federal Tax Partner
- Nicole Berkow, Federal Tax Senior Manager
- Lesa Shoemaker, State and Local Tax Partner
- Brian Trueman, State and Local Tax Director

PwC will make reasonable efforts to maintain continuity of its team members. PwC will assign other team members as needed.

### **IV. FEES, EXPENSES AND PAYMENT**

#### **4.1 Professional Fees and Expenses:**

##### (a) 2023 Tax Compliance Services

PwC's fee for the Services will be \$130,000. All PwC Subcontractor (as defined) fees shall be considered fees and not expenses and are included in the agreed fee.

##### (b) Subsequent Year's Tax Compliance Services

PwC's fee is based primarily on the time required by PwC's professionals to complete the engagement. Amounts billed for Services performed by PwC or the PwC Subcontractors (as defined) shall be considered fees and not expenses and will be billed at rates determined by PwC





Big Lots Stores, LLC  
March 29, 2024

based upon experience, skill and other factors or as otherwise agreed by the parties. Hourly rates may be revised from time to time, and the adjusted rates will be reflected in PwC's billings. All rates will require your prior approval.

In addition to the fees set forth above, PwC will bill Client for reasonable out-of-pocket expenses, including PwC's internal per-ticket charges for coach class airfare, hotel accommodations, and per diem meal expenses incurred by PwC in connection with the Services ("Expenses"), provided that: (i) such Expenses are detailed on an invoice therefore, and (ii) any Expense greater than \$500 is preapproved in writing by Client. Expenses will in no event exceed an amount equal to 15% of the fees charged for the Services in connection with which the Expenses were incurred. You agree to reimburse us for sales, use or value added tax, if applicable, which will be included in the invoices for Services or at a later date if it is determined that such taxes should have been collected. The amount of our fee is based on the assumption that we will receive the information and assistance as detailed in the agreement. In the event we believe an additional fee is required as the result of the failure of Client to meet any of these requests or for any other reason, we will inform you promptly.

In the event of a termination, the total fees due from Client to PwC shall be based on the time spent by PwC professionals on the Services through the date of termination, billed at PwC's hourly rates, except as otherwise provided herein.

#### **4.2 Payment Terms:**

PwC's standard practice is to render invoices on a monthly basis. Payment of PwC's invoices is due on presentation and expected to be received within 60 days of the invoice date.

#### **V. TERM OF THIS SOW**

The term of this SOW will commence on the Project Start Date and end once Services are completed. Either party may terminate this SOW and any Services by giving written notice to that effect to the other party.

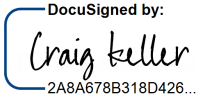
\* \* \* \* \*



Big Lots Stores, LLC  
March 29, 2024

Each of the parties has caused this SOW to be executed on its behalf by its duly authorized representative as of the date first above written.

**PwC US Tax LLP**

By:   
2A8A678B318D426...

Craig Keller, Partner  
(330) 705-0237

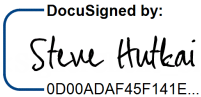
Date: 3/29/2024

**Attachments:**

**Data Protection Exhibit**

Exhibit I - Listing of Returns to be Prepared

**Big Lots Stores, LLC (formerly Big Lots Stores, Inc.), on behalf of itself and its Affiliates**

By:   
0D00ADAF45F141E...

Name: Steve Hutkai

Title: Vice President, Tax & Treasurer

Date: 4/9/2024



Big Lots Stores, LLC  
March 29, 2024

**Exhibit I - Big Lots Stores, LLC (formerly Big Lots Stores, Inc.)**

**Particular Services to be Provided**

**Listing of Returns to be Prepared – Federal and State**

Entity Name	Jurisdiction	Return Form	Paper or Electronic Filing	Filing Method	Return Type
Big Lots, Inc. and Subsidiaries	Federal	Form 1120	E-file	Consolidated	Income
Big Lots, Inc. (#16 DivCon)	Federal	Proforma	N/A	N/A	Income
Big Lots, Inc. (#16)	Federal	Proforma	N/A	N/A	Income
Big Lots Management, LLC (#13)	Federal	Proforma	N/A	N/A	Income
PNS Stores, Inc. (#51)	Federal	Proforma	N/A	N/A	Income
BLM Elims	Federal	Proforma	N/A	N/A	Income
Consolidated Property Holdings (#43 DivCon)	Federal	Proforma	N/A	N/A	Income
Consolidated Property Holdings, LLC. (#43)	Federal	Proforma	N/A	N/A	Income
Broyhill LLC (#44)	Federal	Proforma	N/A	N/A	Income



Big Lots Stores, LLC  
March 29, 2024

Elimination – CPHI Divisional (#33)	Federal	Proforma	N/A	N/A	Income
Big Lots Stores, LLC (DIVCON)	Federal	Proforma	N/A	N/A	Income
Big Lots Stores, LLC (#10)	Federal	Proforma	N/A	N/A	Income
CS Ross Company (#14)	Federal	Proforma	N/A	N/A	Income
Great Basin, LLC (#24)	Federal	Proforma	N/A	N/A	Income
Big Lots eCommerce, LLC (#32)	Federal	Proforma	N/A	N/A	Income
Big Lots F&S, Inc. (#38)	Federal	Proforma	N/A	N/A	Income
CSC Distribution, LLC (#45)	Federal	Proforma	N/A	N/A	Income
Closeout Distribution, Inc. (#47)	Federal	Proforma	N/A	N/A	Income
Durant DC, LLC (#49)	Federal	Proforma	N/A	N/A	Income
AVDC, Inc. (#54)	Federal	Proforma	N/A	N/A	Income
GAFDC, LLC (#70)	Federal	Proforma	N/A	N/A	Income
BLBO Tenant, LLC (#56)	Federal	Proforma	N/A	N/A	Income
PAFDC, LLC (#71)	Federal	Proforma	N/A	N/A	Income



Big Lots Stores, LLC  
March 29, 2024

WAFDC, LLC (#73)	Federal	Proforma	N/A	N/A	Income
INFDC, LLC (#74)	Federal	Proforma	N/A	N/A	Income
ELIMINATION - BLSI (#53)	Federal	Proforma	N/A	N/A	Income
ELIMINATION - BLI (#20)	Federal	Proforma	N/A	N/A	Income
Big Lots F&S, Inc.	Alabama	Form PPT	E-file	Separate	Franchise
Big Lots, Inc. ("BLI") and Subsidiaries	Alabama	Form 20C	E-file	Nexus Consol.	Income
Big Lots Stores, LLC	Alabama	Form CPT	E-file	Separate	Franchise
CSC Distribution, LLC	Alabama	Form PPT	E-file	Separate	Franchise
Great Basin, LLC	Alabama	Form PPT	Paper File	Separate	Franchise
Big Lots Management, LLC	Alabama	Form PPT	Paper File	Separate	Franchise
Big Lots, Inc. ("BLI") and Subsidiaries	Arizona	Form 120	E-file	Unitary	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Arkansas	Form AR1100CT	E-file	Nexus Consol.	Income
Big Lots, Inc. ("BLI") and Subsidiaries	California	Form 100	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Colorado	Form 112	E-file	Unitary	Income



Big Lots Stores, LLC  
March 29, 2024

Big Lots Stores, LLC and Subsidiaries	Connecticut	Form CT-1120	Paper File	Unitary	Income
Big Lots Stores, LLC	Delaware	Form 1100	E-file	Separate	Income
Big Lots, Inc.	Delaware	Form 1100	E-file	Separate	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Florida	Form F-1120	E-file	Consolidated	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Georgia	Form 600	E-file	Nexus Consol.	Income/Net Worth
Big Lots, Inc. ("BLI") and Subsidiaries	Idaho	Form 41	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Illinois	Form IL-1120	E-file	Unitary	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Indiana	Form IT-20	E-file	Nexus Consol.	Income
Big Lots Stores, LLC and Subsidiaries	Iowa	Form IA1120	E-file	Nexus Consol.	Income
Big Lots Stores, LLC and Subsidiaries	Kansas	Form K-120	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Kentucky	Form 720	Paper File	Consolidated	Income
Consolidated Property Holdings, Inc. ("CPHI")	Louisiana	Form CIFT-620	E-file	Separate	Income
Big Lots Stores, LLC	Louisiana	Form CIFT-620	E-file	Separate	Income



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc.	Louisiana	Form CIFT-620	E-file	Separate	Income
Big Lots Stores, LLC and Subsidiaries	Maine	Form 1120ME	E-file	Unitary	Income
Big Lots, Inc.	Maryland	Form 500	E-file	Separate	Income
Big Lots Stores, LLC	Maryland	Form 500	E-file	Separate	Income
Big Lots Stores, LLC and Subsidiaries	Massachusetts	Form 355U	E-file	Unitary	Excise
Big Lots Stores, LLC and Subsidiaries	Michigan	Form 4891	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Minnesota	Form M4	E-file	Unitary	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Mississippi	Form 83	E-file	Nexus Consol.	Income/ Franchise
Big Lots, Inc. ("BLI") and Subsidiaries	Missouri	Form MO-1120	E-file	Nexus Consol.	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Montana	Form CIT	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Nebraska	Form 1120N	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	New Hampshire	NH-1120	Paper File	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	New Jersey	CBT-100U	E-file	Unitary	Income





Big Lots Stores, LLC  
March 29, 2024

Big Lots Stores, LLC and Subsidiaries	New Mexico	CIT-1	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	New York	Form CT-3-A/ CT-3-M	E-file	Unitary	Income
Big Lots Stores, LLC	North Carolina	Form CD-405	E-file	Separate	Income/ Franchise
Consolidated Property Holdings, Inc. ("CPHI")	North Carolina	Form CD-405	E-file	Separate	Income/ Franchise
Big Lots, Inc.	North Carolina	Form CD-405	E-file	Separate	Income/ Franchise
Big Lots Stores, LLC and Subsidiaries	North Dakota	Form 40	E-file	Unitary	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Oklahoma	Form 512	E-file	Nexus Consol.	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Oregon	Form OR-20	E-file	Unitary	Income
Big Lots, Inc.	Pennsylvania	Form RCT-101	E-file	Separate	Income
Big Lots Stores, LLC	Pennsylvania	Form RCT-101	E-file	Separate	Income
Consolidated Property Holdings, Inc. ("CPHI")	Pennsylvania	Form RCT-101	E-file	Separate	Income
Big Lots Stores, LLC and Subsidiaries	Rhode Island	Form RI-1120C	E-file	Unitary	Income



Big Lots Stores, LLC  
March 29, 2024

Consolidated Property Holdings, Inc. ("CPHI") Combined	South Carolina	Form SC-1120	E-file	Nexus Consol.	Income/ Franchise
Big Lots, Inc.	Tennessee	Form FAE 170	E-file	Separate	Franchise/Excise
Big Lots Stores, LLC	Tennessee	Form FAE 170	E-file	Separate	Franchise/Excise
Consolidated Property Holdings, Inc. ("CPHI")	Tennessee	Form FAE 170	E-file	Separate	Franchise/Excise
Big Lots, Inc. ("BLI") and Subsidiaries	Utah	Form TC-20	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Vermont	Form CO-411	E-file	Unitary	Income
Big Lots, Inc. ("BLI") and Subsidiaries	Virginia	Form 500	E-file	Nexus Consol.	Income
Big Lots Stores, LLC and Subsidiaries	West Virginia	Form CIT-120 Form 500	E-file	Unitary	Income
Big Lots Stores, LLC and Subsidiaries	Wisconsin	Form 6	E-file	Unitary	Income

**Listing of Returns to be Prepared - Local**

Entity Name	Jurisdiction	Paper or Electronic Filing	Filing Method	Return Type
Big Lots, Inc. & Subs.	Akron, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc. & Subs.	Alliance, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Ashland, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Athens, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Barberton – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Battle Creek, MI	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Beachwood – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Bellefontaine – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Big Rapids, MI	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Blue Ash, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Boone County BOE, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Boone County MHT, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Boone County Ordinance #430-1A, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Bowling Green, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc.	Bowling Green, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Bowling Green, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Brunswick, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Cambridge, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots Stores, LLC	Campbell County, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Campbellsville (City of), KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Chardon – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Chillicothe, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Circleville – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc.	Coal Run Village, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Columbus, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Coshocton, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Covington, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Danville/Boyle County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Defiance, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Delaware, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Dublin, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Elizabethtown, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Elyria – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Fairfield , OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Findlay, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc.	Frankfort, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Fremont – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Gallipolis, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Garfield Heights – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Georgetown-City, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Georgetown-Scott County Schools. KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Glasgow, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Grove City – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Harrison – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Hartville, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Hazard, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Heath, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Henderson, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Highland Heights – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Holl-Spring. Twp JEDZ – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Hopkins County, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Hopkinsville, KY	Paper File	Separate - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc. & Subs.	Huber Heights, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Jackson, MI	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Kansas City, MO	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Kettering, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Knox County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Lancaster, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Lapeer, MI	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Laurel County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Lebanon, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Lex-Fay BOE, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Lex-Fay Net Profits Tax, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Lorain, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Louisville/Jefferson County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc.	Louisville/Jefferson County, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Madisonville, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Marietta, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Marysville, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots Stores, LLC	Mayfield, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Mentor – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Miamisburg, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Middlesboro, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Middletown, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Milford – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Montgomery County (Mt Sterling), KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Morehead, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Mount Vernon, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Multnomah County/Portland, OR	Paper File	Combined - Local	Income Tax
Big Lots, Inc. & Subs.	Portland Metro Tax, OR	Paper File	Combined - Local	Income Tax
Big Lots, Inc. & Subs.	Portland Clean Energy Surcharge, OR	Paper File	Combined - Local	Income Tax
Big Lots Stores, LLC	Muskegon, MI	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	New Philadelphia, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Newark, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Niles – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	North Olmsted – RITA, OH	Paper File	Consolidated - Local	Income Tax





Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc. & Subs.	Norwalk – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Ontario, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Oregon, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Owensboro, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Paducah (McCracken), KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Parma, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Parma Heights – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Perry County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Pickerington, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Pike County, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Piqua, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Pontiac, MI	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Portsmouth, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Prestonsburg, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Reynoldsburg – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Richmond, KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Riverside – CCA, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc. & Subs.	Rossford, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	Rowan County, KY	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Somerset (Pulaski), KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Springdale, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Springfield, OH	Paper File	Consolidated - Local	Income Tax
Big Lots Stores, LLC	St. Louis, MO	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	St. Marys, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Strongsville – RITA, OH	Paper File	Separate - Local	Income Tax
Big Lots Stores, LLC	Taylor County (Campbellsville), KY	Paper File	Separate - Local	Income Tax
Big Lots, Inc. & Subs.	Tiffin, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Toledo, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Trotwood, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Van Wert, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Wadsworth – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Westerville, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Willoughby – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Wilmington, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

Big Lots, Inc. & Subs.	Wintersville – RITA, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Wooster, OH	Paper File	Consolidated - Local	Income Tax
Big Lots, Inc. & Subs.	Zanesville, OH	Paper File	Consolidated - Local	Income Tax



Big Lots Stores, LLC  
March 29, 2024

**Legend:**

**Entity Name** - Legal name of each filing entity

**Jurisdiction** - Name of federal, state, city, or other taxing jurisdiction

**Return Form** - The form that the return will be filed on.

**Paper or Electronic Filing** - Indicate if PwC will be the Electronic Return Originator (ERO) with respect to the particular form.

**Foreign Entity Forms** - For each filing entity list the number (or name) of foreign entity forms covered by the scope of the engagement and the number of each that will be attached. Client may also list separately the name of the entity and the form associated with the entity. Engagement teams may also wish to break out this listing by affiliates in the case of consolidated returns. This column title may be modified and used to identify other attachments, schedules, or elections as agreed upon with the client. For the Foreign Entity Forms column, the team can put "N/A" if it is not applicable.

**Return Type** - Type or return and/or report (Income, franchise, net worth, annual report, business)

**Filing Method** - Type of filing (separate, combined, consolidated, unitary). Details should be provided when the group filing the return differs from the federal return. (i.e. federal structure less subsidiary C).

If the filing period for the return differs from the federal return, a "Filing Period" column should be added.

**Forms and Statements to be Prepared**

Entity Name	Return Form
Big Lots, Inc. and Subsidiaries	Form 4562 – Depreciation and Amortization
Big Lots, Inc. and Subsidiaries	Form 4797 – Sales of Business Property
Big Lots, Inc. and Subsidiaries	Form 851 – Affiliations Schedule
Big Lots, Inc. and Subsidiaries	Form 1125-E – Compensation of Officers
Big Lots, Inc. and Subsidiaries	Form 2220 – Underpayment of Estimated Tax by Corporations
Big Lots, Inc. and Subsidiaries	Schedule D – Capital Gains and Losses
Big Lots, Inc. and Subsidiaries	Schedule UTP – Uncertain Tax Positions
Big Lots, Inc. and Subsidiaries	Statements and elections as mutually agreed upon

## DATA PROTECTION EXHIBIT

This Data Protection Exhibit (this "**Exhibit**") is made a part of the Statement of Work (the "SOW"), as applicable, to which it is attached, by and between PwC US Tax LLP ("PwC") and Big Lots Stores, LLC (formerly Big Lots Stores, Inc.), for itself and its Affiliates (collectively, "Client"). Capitalized terms used in this Exhibit but not defined herein will have the meanings assigned to such terms in the SOW. This Exhibit sets forth the confidentiality and security requirements for Client Personal Information (as defined below).

**1.** For purposes of this Exhibit, (i) the term "**process**" shall mean any operation or set of operations which is performed upon Client Personal Information, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction; and (ii) the term "**Services**" shall have the meaning set forth in the SOW or, if the SOW does not define "Services", shall mean the services to be performed by PwC as set forth in and pursuant to the SOW.

**2. "Client Personal Information"** shall mean information that relates to an identified or identifiable household or living individual that is provided by or on behalf of Client to PwC in connection with PwC's performance of Services pursuant to the SOW. The categories of data subjects and types of Client Personal Information anticipated to be provided to PwC in connection with the performance of Services are set forth on the attached Schedule A. Client shall not provide PwC with Client Personal Information except as agreed by the parties and set forth in Schedule A. For the avoidance of doubt, Client Personal Information shall not include any information that has been anonymized such that the data no longer relates to an identified or identifiable household or living individual.

**3.** PwC and Client shall process Client Personal Information in accordance with applicable data protection laws, rules, and regulations, including without limitation and in each case to the extent applicable, the California Consumer Privacy Act of 2018 (the "**CCPA**"), the California Privacy Rights Act of 2020 (the "**CPRA**"), and similar state laws (collectively, "**Applicable Data Protection Laws**") and PwC shall process Client Personal Information only in accordance with Client's documented instructions as established in or provided in accordance with this Exhibit (including, without limitation, Schedule A) and/or the SOW.

**4.** PwC is acting as a service provider (as such term is defined by the CCPA) to Client in connection with PwC's performance of Services pursuant to the SOW. PwC acknowledges and confirms that it does not provide Client with any monetary or other valuable consideration in exchange for Client Personal Information and certifies that it understands and will comply with the restrictions set forth in this Section 4. Except as required by applicable law, regulation, or professional standard, PwC will not collect, access, use, disclose, process, or retain Client Personal Information for any purpose other than the purpose of performing the Services or another business purpose permitted by 11 CCR § 999.314(c), this Exhibit, or the SOW. In particular, PwC shall not sell (as defined by Applicable Data Protection Laws, including without limitation and to the extent applicable, the CCPA) or share (as defined by the CPRA) any Client Personal Information. PwC will, to the extent legally permissible, notify

Client if PwC receives a request from a data subject of Client Personal Information seeking to exercise such data subject's rights under Applicable Data Protection Laws ("**Data Subject Access Request**"), and will, on Client's reasonable request, provide reasonable assistance in connection with Client's response to such Data Subject Access Request.

5. Client shall provide PwC with prior written notice if it intends to provide PwC with access to "**Protected Health Information**" as defined in the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations. If PwC agrees to process such Protected Health Information, then Client shall not provide Protected Health Information and PwC shall not commence such processing unless and until a Business Associate Agreement, in a form acceptable to both parties, has been executed and is effective between the parties.

6. The parties acknowledge that PwC does not maintain compliance with the Payment Card Industry Data Security Standard ("**PCI DSS**"), and Client therefore agrees that it will not provide PwC, directly or indirectly, with access to any payment card information, including without limitation any information relating to a payment card transaction except to the extent such access: (i) is expressly agreed upon in the Agreement; and (ii) occurs solely at a Client facility utilizing Client computing devices.

7. PwC shall ensure that persons authorized by PwC to process Client Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Without limiting the foregoing, except as otherwise permitted under this Exhibit or the SOW, PwC shall limit access to Client Personal Information to the Beneficiaries who require such access in order to perform the Services or to comply with applicable law or professional standards. PwC shall be solely responsible for all Client Personal Information provided to the Beneficiaries. For purposes of this Exhibit, the term "**Beneficiaries**" shall mean the PwC Subcontractors and the partners, principals, members, and employees of PwC and the PwC Subcontractors.

8. For purposes of this Exhibit, "**PwC Sub-Processor**" means a PwC Subcontractor engaged to process Client Personal Information on behalf of Client in connection with such PwC Subcontractor's performance of Services. Client hereby grants PwC general written authorization to engage the PwC Sub-Processors set forth in Schedule A. PwC shall inform Client of: (i) any changes concerning the addition or replacement of Other PwC Firms by updating the hyperlink set forth in Schedule A. If Client notifies PwC in writing of any objections to such changes, PwC shall work with Client in good faith to find a commercially reasonable, mutually agreeable resolution to such objection. Without limiting the foregoing, Client also agrees that PwC may provide information PwC receives in connection with the SOW, including without limitation Client Personal Information, to: its subsidiaries and affiliates; the Other PwC Firms, including those listed at the hyperlink set forth in Schedule A; and other PwC Subcontractors for internal, administrative, and/or regulatory compliance purposes as permitted under the SOW. For a list of the primary PwC Subcontractors who provide back-office and administrative support to PwC, please visit <https://www.pwc.com/us/en/site/privacy.html>. PwC shall require the PwC Subcontractors, including without limitation the PwC Sub-Processors, who are provided access to, or otherwise come into contact with, Client Personal Information to protect all such Client

Personal Information according to terms substantively similar to the terms of this Exhibit. PwC will be solely responsible for the protection of any Client Personal Information provided to the PwC Subcontractors, including without limitation the PwC Sub-Processors, and for compliance with this Exhibit.

**9.** PwC will implement and maintain the security controls set forth at Schedule B, which are designed to comply with Applicable Data Protection Laws and protect against the unauthorized or unlawful processing, accidental loss, destruction, or damage of information such as Client Personal Information. Client acknowledges that PwC may change the security controls through the adoption of new or enhanced security technologies, provided that such changes do not diminish the level of security of Client Personal Information in PwC's possession, custody, or control, and Client authorizes PwC to make such changes.

In no way limiting the generality of Section 9 of this Exhibit, at a minimum, the Safeguards must be designed to include: (i) limiting access to authorized persons; (ii) implementing network, device application, database and platform security, including network firewall provisioning and intrusion detection, the timely application of patches, fixes and updates to operating systems and applications as necessary and based on risk severity; (iii) securing information transmission, storage and disposal; (iv) implementing authentication and access controls within PwC's media, applications, operating systems and equipment; (v) physically and/or logically segregating Client data from PwC's own information and that of third parties so that Client data is not commingled with any other types of information; (vi) implementing appropriate security and integrity procedures and practices for inclusion on the list of authorized persons, including, but not limited to, conducting background checks consistent with Applicable Law; and (vii) encrypting Client Personal Information at rest on laptops, smartphones, external media storage, and backups, and in transit: (A) using recognized industry standards and a commercially supported encryption solution; (B) where possible, changing the data encryption keys at a minimum once per calendar year; (C) storing the encryption keys in a secure location with limited access; and (D) and maintaining a list of which authorized persons are encryption key holders, restricting access to only those indicated authorized persons, and reviewing the appropriateness of the indicated authorized persons at least once per quarter; and (viii) ensuring that Client data, other than Client Personal Information, is transmitted in a mutually agreed upon secure manner. Contractor further agrees that Client Data will not be Processed on any portable or laptop computing devices or any portable storage medium, unless the Client Data Processed thereon is encrypted at rest and in transit over public or wireless network, using an encryption solution that aligns to industry standards. To the extent PwC receives or accesses any information in a deidentified or aggregated form, PwC will make no attempt to identify any individual to whom such information relates and will take commercially reasonable measures to prevent such reidentification of the information. PwC will promptly notify Big Lots if any Contractor Facilities & Systems do not conform to the standards set forth in Sections 9 of this Exhibit.

**10.** PwC shall make available to Client all information necessary to demonstrate PwC's compliance with the obligations laid down in this Exhibit and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client that is not a PwC competitor. For the avoidance of doubt, the audits and inspections described in the preceding sentence shall be conducted solely as follows: on Client's written request, not



more than once annually or if there are indications of non-compliance, in each case during the term of the SOW, PwC will: (i) accurately complete a written security and privacy assessment questionnaire related to the Services, provided that doing so does not violate applicable law or PwC's confidentiality obligations, meet with Client to discuss the results of the assessment and answer questions regarding PwC's information security program, and reasonably treat any noted assessment deficiencies based upon risk severity; and/or (ii) provide PwC's then-current SOC3 audit report for its U.S. data center around AICPA trust principles of security and availability.

**11.** Client represents that it shall comply with Applicable Data Protection Laws and acknowledges and agrees that, as between the parties, Client is responsible for providing any required notices to, and/or obtaining any required consents or authorizations from, data subjects of the Client Personal Information and/or regulatory authorities, as applicable, in connection with Client Personal Information.

**12.** PwC will notify Client within 72 hours of discovering accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Personal Information in its possession that is in breach of this Exhibit (a "**Security Incident**"). PwC will give Client notice of a Security Incident by phone at 614-395-2821, leaving a voicemail if there is no response, and email to [privacy@biglots.com](mailto:privacy@biglots.com), or such other phone number or email address as provided by Client from time-to-time. PwC shall take reasonable steps to mitigate the effects of, and to minimize any damage resulting from, such Security Incident. At Client's reasonable request and subject to applicable law and PwC's confidentiality obligations, PwC agrees to meet with Client to discuss, as applicable and available at the time, the procedures that were followed during the investigation of any Security Incident, the chain of custody information, the forensic analysis of event logs used to determine the root cause, any restoration of data that may be required, and the remedial/corrective actions to be taken to prevent the Security Incident from occurring again. In the event of a confirmed Security Incident involving unencrypted Client Personal Information, subject to the applicable limitations of liability as set forth in the Agreement, if any, PwC shall reimburse the Client for the cost of providing individuals affected by unauthorized disclosure and/or misuse of the Client Personal Information with notification of the Security Incident.

**13.** On Client's written request at termination or expiration of the SOW, PwC shall, where feasible, promptly and securely destroy and confirm such destruction of all Client Personal Information in its possession or control (including, without limitation, all electronic copies such as on hard drives, backup tapes, portable devices, optical, magnetic, or other storage media, as well as all hard copies) or, at the request and cost of Client, return such Client Personal Information in its possession or control, delete existing copies thereof, and confirm such destruction. Notwithstanding the foregoing, PwC shall be permitted to retain copies of Client Personal Information consistent with its document retention policies or as required by applicable law, regulation, or professional standards. Any Client Personal Information so kept shall be maintained in accordance with PwC's obligations under this Exhibit and only processed to the extent and for as long as required for such purposes.

### **Schedule A - Data Protection Exhibit**

#### **DESCRIPTION OF TRANSFER**

- a. Categories of data subjects (e.g., current and/or former employees of Client) whose Client Personal Information is provided to PwC in connection with its performance of the Services:
  - Employees of this client
- b. Categories of Client Personal Information (e.g., Social Security Numbers, dates of birth, or home addresses) provided to PwC in connection with its performance of the Services:
  - Business contact information commonly referred to as “business card data” such as name, title, email, office address and office phone number (excluding data collected for the purposes of corresponding with clients, suppliers or JBR partners during the course of a project)
- c. Sensitive data transferred (if applicable): None, except to the extent expressly agreed by the parties in this Schedule A or the applicable Statement of Work. For this purpose, "sensitive data" means Client Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.
- d. Frequency of the transfer (e.g., whether the Client Personal Information is transferred on a one-off or continuous basis): As needed to facilitate performance of the Services in accordance with the SOW.
- e. Nature and purpose(s) of the processing:
  - i. When PwC processes Client Personal Information as a controller, PwC shall do so for the purposes of: (i) providing the Services; (ii) administering, managing, and developing PwC's business and services; (iii) security, quality, and risk management activities; (iv) providing Client with information about PwC and its range of services; and/or (v) complying with any applicable requirement of law, regulation, or professional standards.
- f. Period for which the Client Personal Information will be retained: Until such Client Personal Information is returned or destroyed in accordance with and subject to the terms of this Exhibit.
- g. PwC may engage the following PwC Sub-Processors in accordance with the terms of this Exhibit and the SOW:
  - i. PwC's subsidiaries and affiliates and the Other PwC Firms, including those listed at <https://www.pwc.com/gx/en/about/office-locations.html>.
  - ii. Independent contractors who are natural persons acting under PwC's supervision.

- iii. Additional PwC Subcontractors engaged to perform Services as permitted under the SOW.

# Security Statement

## PwC Information Security Policy (ISP)

Version: 6.0

Data classification: **Public**

July 2023



# Contents

Introduction	4
Scope	5
Security policy	6
Security organisation	7
PwC personnel responsibilities	8
Access controls	9
Cyber security incident management	11
Data protection	12
Service management	13
System development	15
Resilience	16
Compliance programme	17
Appendix A – Common terms and definitions	18

## Document history

Version	Date	Changes made	Author(s)
1.00	September 2017	Initial Publication	ISRC Team
1.01	August 2018	FY19 review. Minor edits for consistency.	ISRC Team
2.00	July 2019	FY20 review. Minor edits for consistency.	IT GRC Policy Team
3.00	July 2020	FY21 review. Minor edits for consistency.	IT GRC Policy Team
4.00	September 2021	FY22 review.	IT GRC Policy Team
5.00	October 2022	FY23 review. Minor edits for consistency.	IT GRC Policy Team
6.00	July 2023	FY24 review.	IT GRC Policy Team

Template version: 1.3

# Introduction

Information Security is a high priority for the PricewaterhouseCoopers (PwC) Network. PwC Member Firms are accountable to their people, clients, suppliers and other stakeholders to protect information that is entrusted to them. Failure to protect information could potentially harm the individuals whose information Member Firms hold, lead Member Firms to suffer regulatory sanctions or other financial losses and impact the PwC reputation and brand. The Information Security Policy outlines the minimum security requirements with which every Member Firm must comply.

The PwC Information Security Policy (ISP) has been developed to safeguard the confidentiality, integrity, and availability of the information and technology assets used by the PwC member firms and is aligned with ISO/IEC 27002:2013 Information technology - Security techniques Code of Practice for Information Security Management industry standard.





# Scope

The Information Security Controls Standard applies to all PwC member firms for all information and systems. It is the policy of the PwC network that the information assets of the member firms be protected from internal or external threats, whether deliberate or accidental, such that:

- Data subject rights are respected.
- Confidentiality of information is maintained.
- Integrity of information can be relied upon.
- Information is available when the business needs it.
- Relevant statutory, regulatory, and contractual obligations are met.
- The PwC brand is protected.

The PwC Information Security Policy (ISP) serves to be consistent with best practices associated with organisational Information Security management. The PwC ISP is aligned with the ISO 27002 standard and tailored to the PwC policy framework.

The purpose of this statement is to provide PwC clients and prospective clients with a high-level overview of the security controls in the PwC ISP.

1. **Security Policy** – describes the need to protect each PwC member firm's information and technology assets and to comply with regulatory and contractual obligations and PwC policies, standards and local security policies.
2. **Security Organisation** – the management of security within PwC, encompassing the PwC network-wide security model framework; third party access to a PwC member firm's resources and security requirements for outsourced service providers.
3. **PwC Personnel Responsibilities** – areas affecting personnel security within a PwC member firm such as employee vetting, terms and conditions of employment, confidentiality agreements, and user awareness training.

4. **Access Controls** – assigning correct and appropriate access to each PwC member firm's information and technology assets based upon a data classification scheme and assigned roles and responsibilities.
5. **Physical and Environmental Security** – building access control, clear desk policy, laptop security – with the overall aim of protecting each PwC member firm's business premises and the information and technology assets that reside within them.
6. **Cyber Security Incident Management** – controls that each PwC member firm is expected to implement to minimise the impact to PwC member firms, in the event of a security breach.
7. **Data Protection** – classification and security of a PwC member firm's information assets and systems, including data classification.
8. **Service Management** – secure operation and management of information processing centres. For example, clear separation of test and production environments, separation of operational duties based upon roles, strong change management controls, and secure network connections.
9. **Systems Development** – development and ongoing maintenance of information systems to include adequate security controls during the conceptual design phase.
10. **Resilience** – business continuity and disaster recovery planning based upon service level agreements and recovery time objectives with the overall aim of minimal impact to the PwC member firm's business in the event of a disaster.
11. **Compliance Programme** – outlines controls that measure and monitor compliance of the PwC member firm's enterprise and systems with the ISP and other relevant security controls as agreed via the policies and standards process. Includes additional controls required to determine compliance with applicable regulations and legislation such as data protection.

# Security policy

The member firms operate within an increasingly electronic, interconnected, and regulated environment that necessitates a consistent and standardised approach to securing information and member firm assets. The PwC ISP Framework is composed of a set of hierarchical cross-referenced documents which cascade down from the security policy statements contained in this document. These statements are used to communicate management's expectations for the key information security principles across PwC.

The ISP Framework will adapt to the changing landscape with continuous improvements to address emerging risks and business needs. The Network Information Security organisation will coordinate an annual review of the PwC ISP Framework and publish amendments in accordance with the defined PwC ISP governance procedure.

The PwC ISP Framework is aligned and compatible with financial services industry recognised security frameworks (e.g., ISO 27002:2013) and best practices. An annual review of alignment and these processes is conducted as part of the governance procedure.

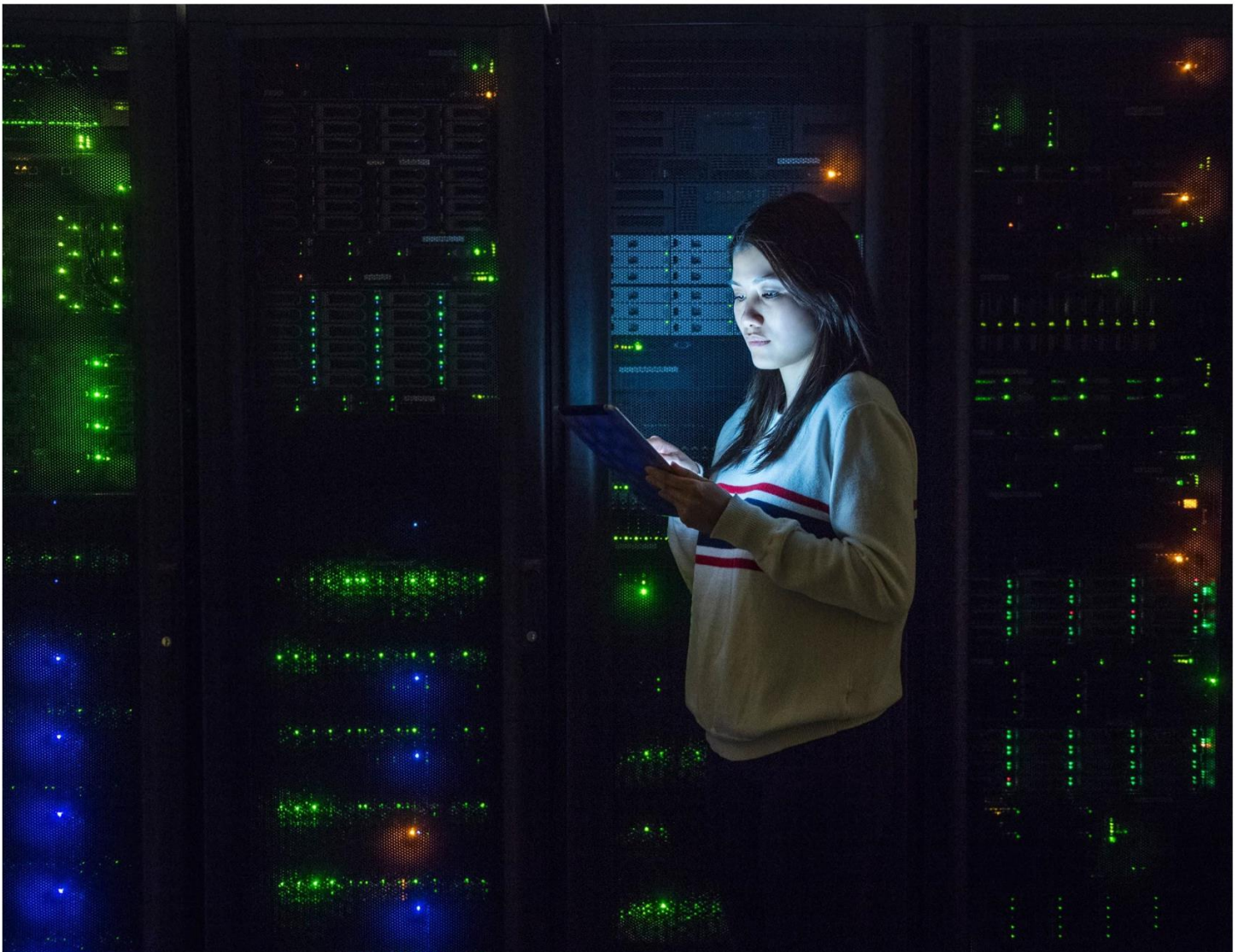
All member firms and information technology resources connected to the PwC network must comply with the PwC ISP, controls and supporting standards that are designed to establish the controls necessary to protect information assets. Any deviation requires risk evaluation that includes identification of mitigating or compensating controls and a formal tracking of exceptions in accordance with the PwC Network Information Security issue management process.



# Security organisation

Clearly defined roles and responsibilities are crucial to develop and deliver a successful information security and Cyber Readiness Programme. The PwC Network Information Security organisation is organised at a network and region/sub-cluster/territory level to effectively manage and execute the information security objectives.

These information security functions across PwC must establish, implement, maintain and enforce PwC's ISP to protect information and member firm assets through the development and implementation of information security services.





# PwC personnel responsibilities

## Human resources security

PwC personnel are the first line of defence in protecting and securing information and Member Firm assets.

Member firms are required to provide training and guidance to all PwC personnel regarding how to be responsible with use of technology and tools. PwC personnel are accountable for complying with the ISP Framework and must always report any suspected violations through the appropriate reporting process.

## Security responsibilities

PwC member firm staff connected to the PwC network must conduct themselves in a manner consistent with PwC's Code of Conduct and operate in compliance with their responsibilities defined in the ISP Framework and relevant standards at all times (for example, on premises, at clients, or working remotely).

## Security and privacy awareness training

PwC member firms provide regular security and privacy awareness training to personnel that must be completed within the timeframes specified. New PwC personnel are required to agree to abide by security and privacy policies. PwC firms are encouraged to periodically distribute newsletters and other communication methods to reinforce security awareness.

## Background checks

To the extent permitted by applicable laws and regulations, PwC member firms screen all prospective personnel prior to making an offer of employment. These checks vary by country but may include financial profile, education, professional licenses and employment verification.

## Confidentiality agreements

Where permitted by law and in accordance with local firm policy, confidentiality agreements (for example non-disclosure agreements) may be implemented and signed by PwC member firm staff and third party suppliers as a condition of employment.

## Appropriate use

Use of electronic communication tools, the internet and portable computer devices is permitted and encouraged where such use supports the goals and objectives of the business. PwC personnel are responsible for proper use of these technologies to protect information and member firm assets.

PwC maintains its own and respects others' intellectual property rights, which includes third party software. PwC personnel have a responsibility to the firm and clients to comply with rules for use of PwC and third party intellectual property and protect creative ideas, innovations or inventions.

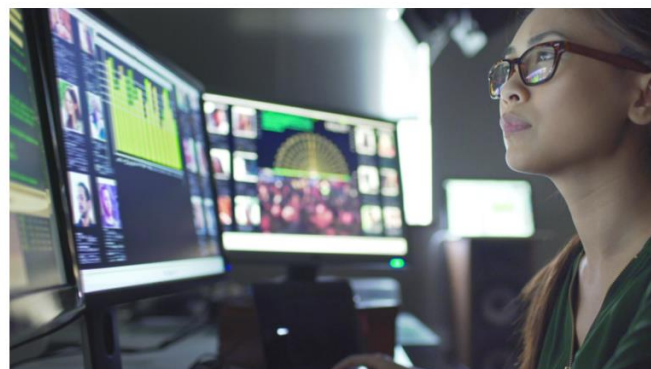
PwC member firms deploy and regularly update web traffic filtering software to block access to inappropriate websites from the PwC network. The PwC member firms must also establish and maintain email gateway service that supports spam-blocking and anti-virus software for attachments.

## Secure printing

PwC member firm staff and third party suppliers must use appropriate authorisation controls available on fax and printer equipment when printing and sending confidential materials.

## Termination processes

PwC member firms document their termination process, including their process for collection of information assets and removal of access rights for departing personnel.



# Access controls

Strong access controls reduce the risk of accidental or deliberate modification or destruction of data as well as protecting against unauthorised access or dissemination.

Access to information must be commensurate with an individual's business role and the least privilege concept, where the minimum access levels are granted based upon their required business needs and the nature of the information they are trying to access. Privileged access must be properly authorised and limited to a defined duration with adequate monitoring and oversight.

## Authorization and authentication controls

Access credentials must uniquely identify an individual and access permissions must be the minimum levels required to perform a user's specific job responsibilities. Access credentials are used to identify the individual and correlate that individual with any related activity performed for which they will be held accountable and responsible. Credentials, therefore, must not be shared or compromised.

Proper business approval must be documented prior to the creation of an individual account or access provisioning. Access must be reviewed upon a change in job responsibility and on a periodic basis, at least annually. Access must be removed immediately upon termination.

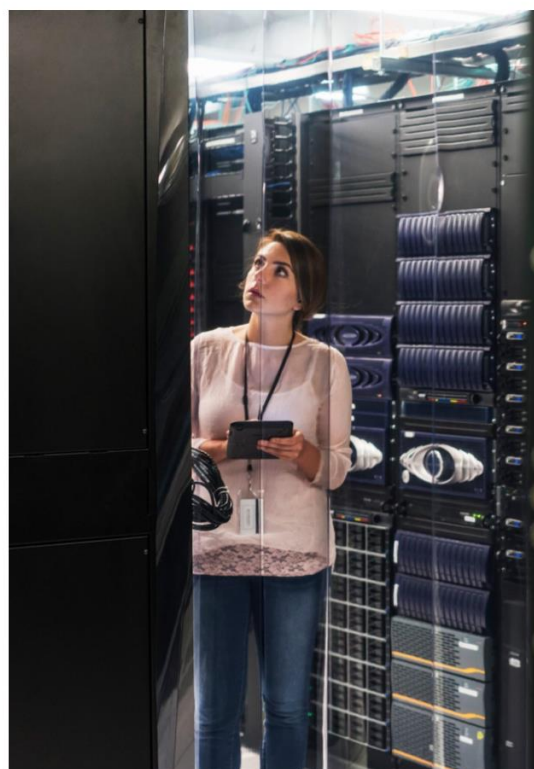
Authentication mechanisms such as login ID and password are the primary means of protecting access to systems, applications and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents unauthorised access. It is mandatory to implement authentication mechanisms commensurate with the level of security risk.

## Privileged access

Privileged access provides permissions to a network, system or application that results in higher risk functions and requires additional controls to mitigate those risks. Privileged access must be kept to a minimum to limit the risk of cyber attacks. Privileged access requests must be individually approved, periodically reviewed and documented with business justification.

## Password requirements

Passwords are the most frequently utilised forms of authentication and when shared with user identification information are classified as highly confidential and protected accordingly. Passwords must be constructed with complexity requirements enforced to reduce the risk of unauthorised access to systems and applications. Stronger password control requirements must be implemented where there is higher security risk associated with the access.



## Remote access

PwC provides personnel with the facilities and opportunities to work remotely to meet client demand or business needs as appropriate. Each member firm must make any user authorised to work remotely aware of the acceptable use of portable computer devices and remote work rules. PwC member firms use virtual private network (VPN) technology through a secure encrypted communications channel where users are required to authenticate using two-factor authentication.

External connections with the PwC networks can leave the network vulnerable to unauthorised access. External perimeter access controls must be implemented based on the risk related to the external connection and be managed with the proper levels of authorisation, oversight and restrictions. In particular, all inbound connections must be terminated in an approved network protected area.

### **Laptop security**

Laptops and workstations expose the organisation to a variety of risks that include points of entry from external sources that could introduce malware or other threats to the firm. In addition to user awareness and training, automated controls that include hard drive encryption must be utilised to further secure endpoints and protect confidential information and related member firm assets.

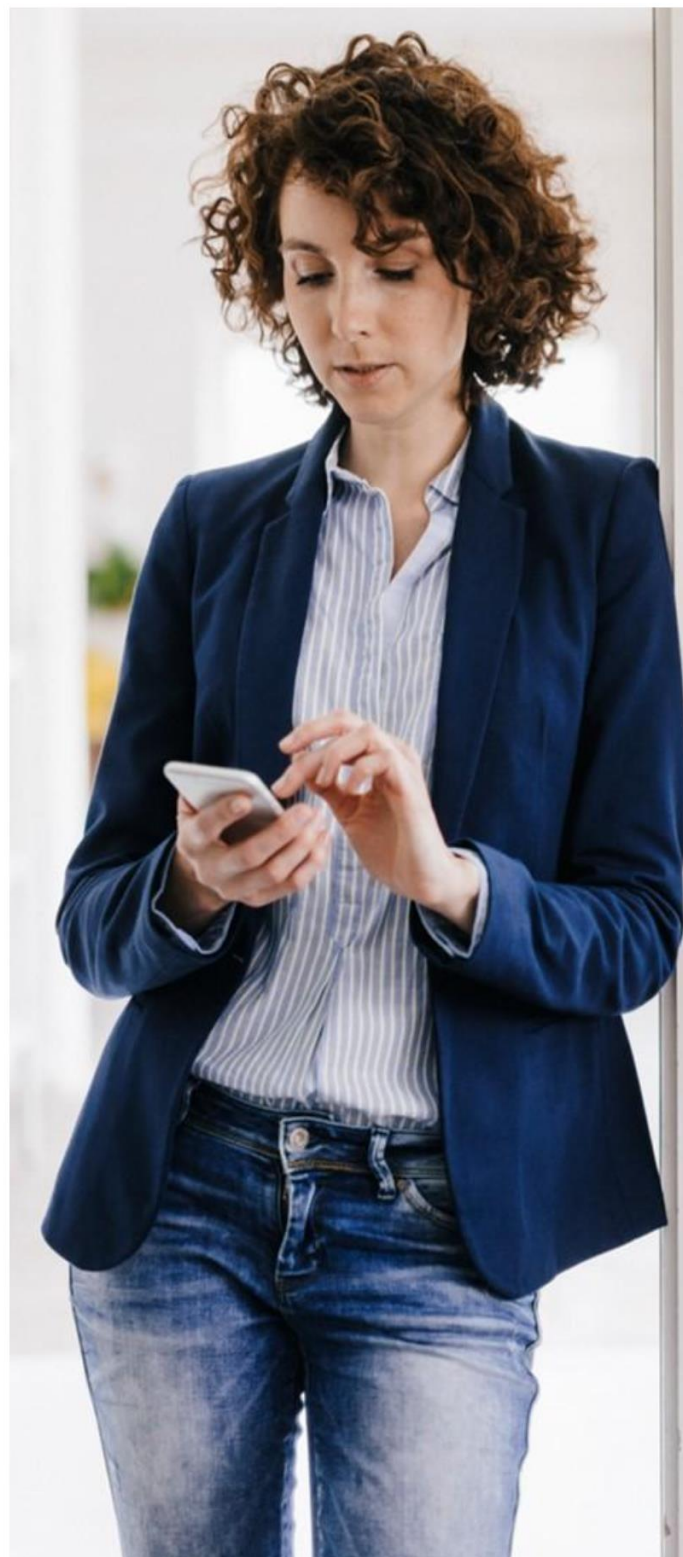
### **Mobile devices**

Mobile computing devices must be configured and fully managed with adequate controls implemented to protect from unauthorised disclosure, loss and theft of confidential information in a member firm's possession, including information belonging to a member firm client and any confidential business information of parties PwC member firms conduct business with.

### **Physical and environmental security**

Physical access is a necessary control to protect computing equipment and confidential information that resides in firm buildings, critical processing centres and all hosting or storage facilities. Physical access to buildings and critical processing centres must be restricted to authorised personnel with a legitimate business need in order to protect against theft, business interruption and unauthorised access to data.

PwC network service delivery, service processing and data centres are designed and constructed with site security as a priority, a tiered approach to physical access control, access limited to authorised personnel and appropriate environmental controls.





# Cyber security incident management

PwC recognises that security incidents are disruptive and may cause damage to individuals, clients or the business function. PwC must be prepared to combat these threats and quickly respond to prevent impacts that may result in financial, legal or reputational implications. In order to be properly prepared, an incident management programme must be implemented to identify, classify, escalate, respond and resolve security incidents in a timely manner and reduce impact to the individuals and the business.

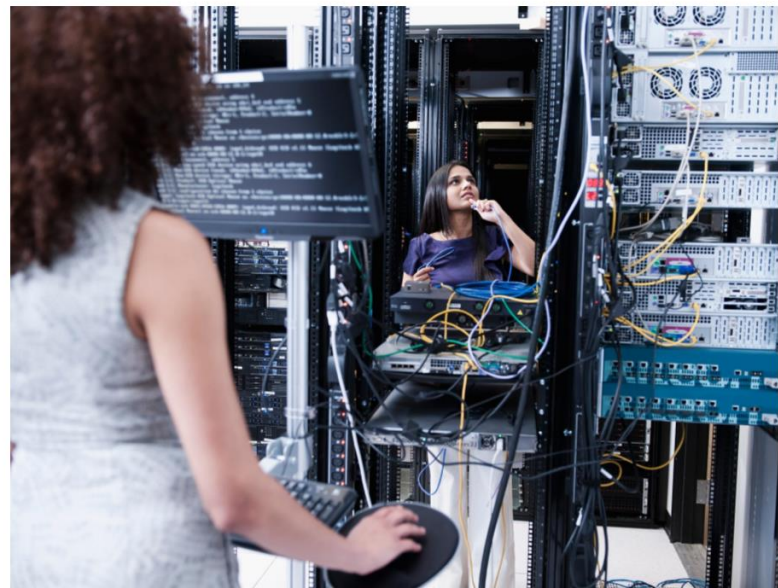
Adequate controls must be implemented to properly detect and defend the firm against malicious software designed to disrupt computer operations. To keep up with the changing threats, encryption methods and up-to-date malware protection software must be implemented to protect data on servers, workstations, laptops, mobile and removable devices.

Detection or suspicion of a security incident is critical for early identification and containment of the impacts of a security incident. PwC personnel must be familiar with the process and points of contact to report and escalate any suspected violation or perceived security incident.

## Network and system monitoring and logging

Monitoring, logging, scanning or other security utilities are necessary with detection of network or system vulnerabilities. All security, audit and system tools must be configured, registered and protected with restricted access privileges, including output that is considered confidential and must be secured in accordance with PwC policy and procedures.

Monitoring and logging are detective controls to identify unexpected system activity that may include a decline in expected system performance or unauthorised activity. Early identification provides support teams with warning indicators of system performance trends that can be addressed to ensure system availability. Appropriate monitoring and logging of systems, applications and networks provide a tracing capability; combined with proper levels of recording of activity, these controls are critical for the containment and remediation process. In addition, filtering and monitoring controls for ingress and egress points prevent malicious activities, cyber attacks, data leaks and other harmful events.



# Data protection

PwC gathers and generates, stores and processes large amounts of data of varying levels of sensitivity during the course of its business. The confidentiality, integrity, and availability of information and information systems is critical to uninterrupted operations and timely provision of services. To accomplish this, member firms implement data management procedures to identify, classify and inventory data with the respective information owner.

Data management procedures must clearly define relevant stakeholders (for example, information owner, information custodian, data privacy/protection officer), data classifications based upon potential business impact of unauthorised access and data lifecycle management (for example, retention, destruction, discovery, user education).

Data must be identified based on data classification and confidentiality requirements and must be protected with use of encryption where appropriate (for example, at rest, during transmission) and consider compliance with local and international laws.

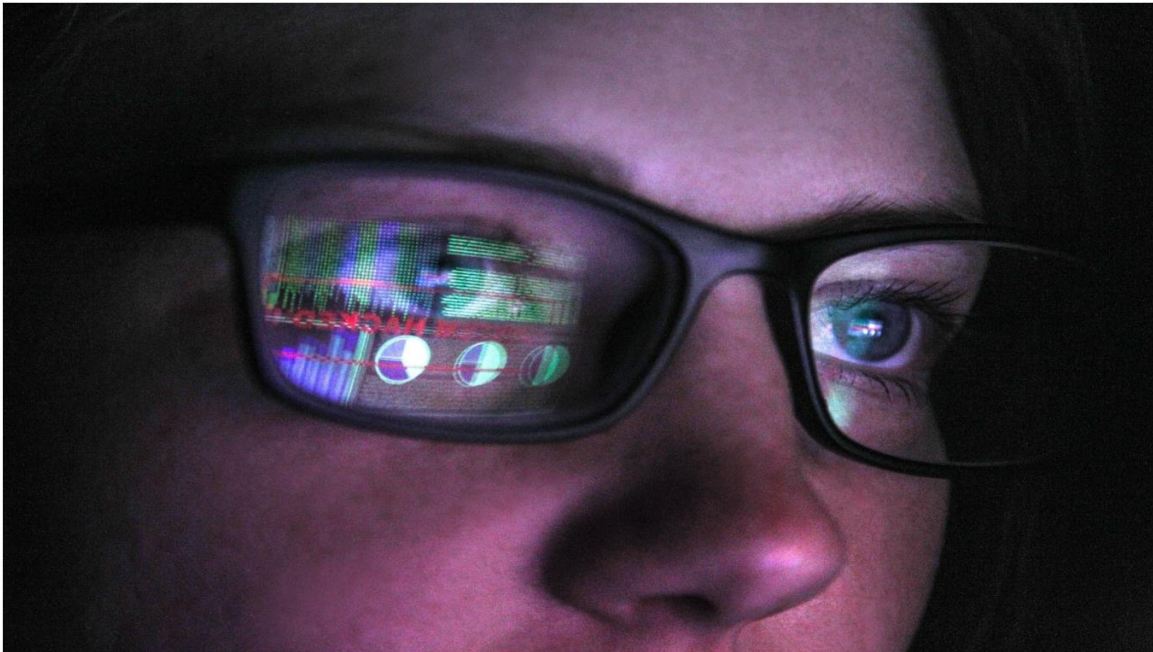
## **Data loss prevention and removable media**

When implemented with appropriate security controls, data loss prevention helps limit the exposure of confidential information. PwC member firms must comply with data loss prevention controls for removable media, email, secure instant messaging, file sharing, web browsers and other technologies. Devices must be configured to prevent writing to unapproved removable media.

## **Retention, disposal and destruction of data and technology equipment**

A retention schedule defines how long business records must be retained and organises records (for example, paper, electronic, other media) based on data classification. Member firms must implement appropriate controls for handling each data classification.

Member firms must also implement control procedures for disposal and destruction of data and technology equipment. Controls must comply with business, legal and regulatory requirements.





# Service management

Effective delivery of information technology services must be aligned to the organisation and security strategy.

PwC maintains various types of technology assets to provide automation to improve processes, strengthen controls, and enable the business and client delivery teams. To protect these assets, baseline security configuration standards are important for the implementation of network devices, databases, servers, user endpoints, mobility devices and cloud computing. Equivalent controls are required when introducing automated solutions or technology from third party suppliers into the PwC network. Additional monitoring and logging controls are used to provide risk identification and audit tracking to protect data and the PwC brand.

## Internal network

The PwC internal network is used to bring together technology with business processes that enables the operations of PwC; it is imperative that the network be procured, configured, secured and monitored accordingly. All network devices, servers, workstations, laptops and mobile devices must be properly procured and installed or configured with appropriate security controls in place to secure against unauthorised access and comply with technology build and support standards. Adequate controls must be implemented when outsourced to ensure proper service level agreements are implemented and asset maintenance is in compliance with any manufacturer or software provider service agreements.

Network security devices that enable production systems must have configuration standards and change management procedures that are documented, readily available and inspected for compliance on a regular basis. All access to the PwC network from a non-PwC location must be monitored for intrusion detection and prevention.

PwC member firms protect network diagrams, network devices, routers, diagnostic equipment or other equipment accordingly and ensure these are accessible only by authorised personnel.

## Wireless networks

Only approved and managed wireless networks are permitted to connect to the PwC network. Wireless access security controls must include centrally managed standards for encryption and authentication.

## Database environments

Databases are the central repository for storage of most confidential data and as such require security control configuration and administration procedures. Non-production databases must be separated from production and relevant controls must be implemented to protect any confidential data stored.

## Cloud computing

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. Cloud computing must have adequate controls implemented to protect personal data and confidential information in a member firm's possession, including personal data and confidential information belonging to a member firm client and any confidential business information of third parties with whom member firms conduct business. Cloud services must undergo security review and risk assessments following the same conditions as newly deployed applications.

## Third party suppliers

PwC member firms leverage the expertise and relationships of third party suppliers for services and solutions that enable client delivery, supplement processes and create efficiencies. PwC must identify and assess security risks during third party supplier selection, engagement and ongoing service delivery. Security risks identified against the PwC ISP Framework must have business risk acceptance as defined in the ISP issue management process and mitigating or compensating controls implemented where legally permissible.

Third party suppliers that require access to IT resources must agree to establish and maintain PwC defined third party security controls and allow the PwC contracting firm, or its authorised representative, the right to audit against the agreed security controls or review existing audit results.

**Technology asset inventory**

Member firms are required to use a centralised inventory tool and maintain an inventory of technology assets, applications, data, and business process information related to the assets.

**Vulnerability and patch management**

PwC reviews vulnerabilities, patches and fixes in order to determine risk and the relative priority for patch deployment in accordance with the PwC security policy. Member firms must implement procedures that include appropriate approvals, timely identification, reporting and treatment of vulnerabilities.

# System development

## Formal system development

PwC member firms follow a secure system development lifecycle (SDLC) with formal documentation that includes appropriate levels of approval and oversight. This enforces implementation of secure system development methodologies and standards as well as proper change management procedures to identify, track, validate and approve changes before being implemented in production.

## Application security reviews

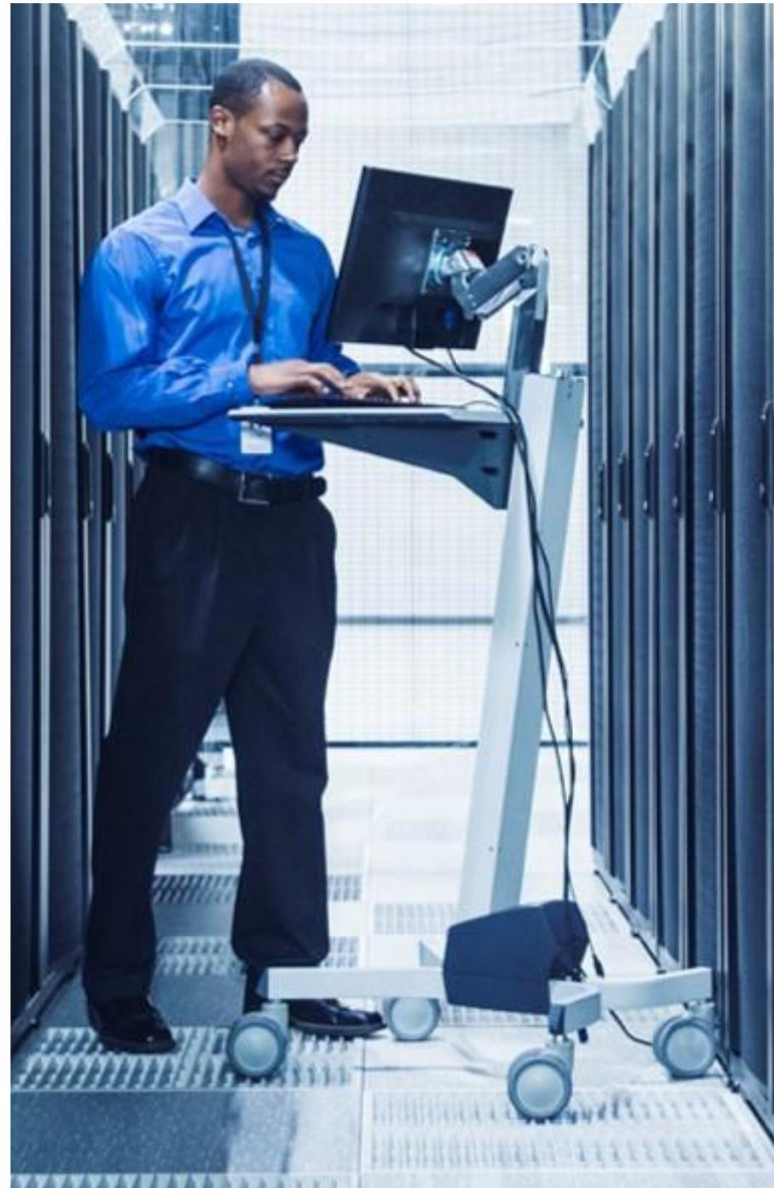
Application development practices must use security and privacy/data protection by design principles to identify and mitigate software vulnerabilities and protect the information stored. The level of security controls implemented (for example, code review, security scans, penetration and vulnerability tests) must be commensurate with the application risk assigned as part of a formal risk assessment.

## Development environments

PwC member firms maintain separate development and production environments and establish procedures that require the use of a change control process to transfer changes from development to production.

## Capacity management

PwC member firms create and maintain capacity management plans and review capacity-planning reports periodically.



# Resilience

PwC is prepared with an effective disaster recovery and business continuity plan to respond to unplanned events or crises. This planning is an effective risk mitigation to minimise business interruption.

PwC member firms maintain business continuity programmes that evaluate potential events and respond to actual events to minimise disruption to services. They have dedicated recovery teams to develop, maintain and periodically test processes and procedures related to business continuity and disaster recovery planning. PwC member firms' IT disaster recovery plans should include a business impact analysis, business continuity and disaster recovery plans, testing, audit, backup approach, training and awareness.

## System backup

Systems are routinely backed up for disaster recovery purposes. Backup removable media must be encrypted, transported securely, stored in a secure location and clearly identified.



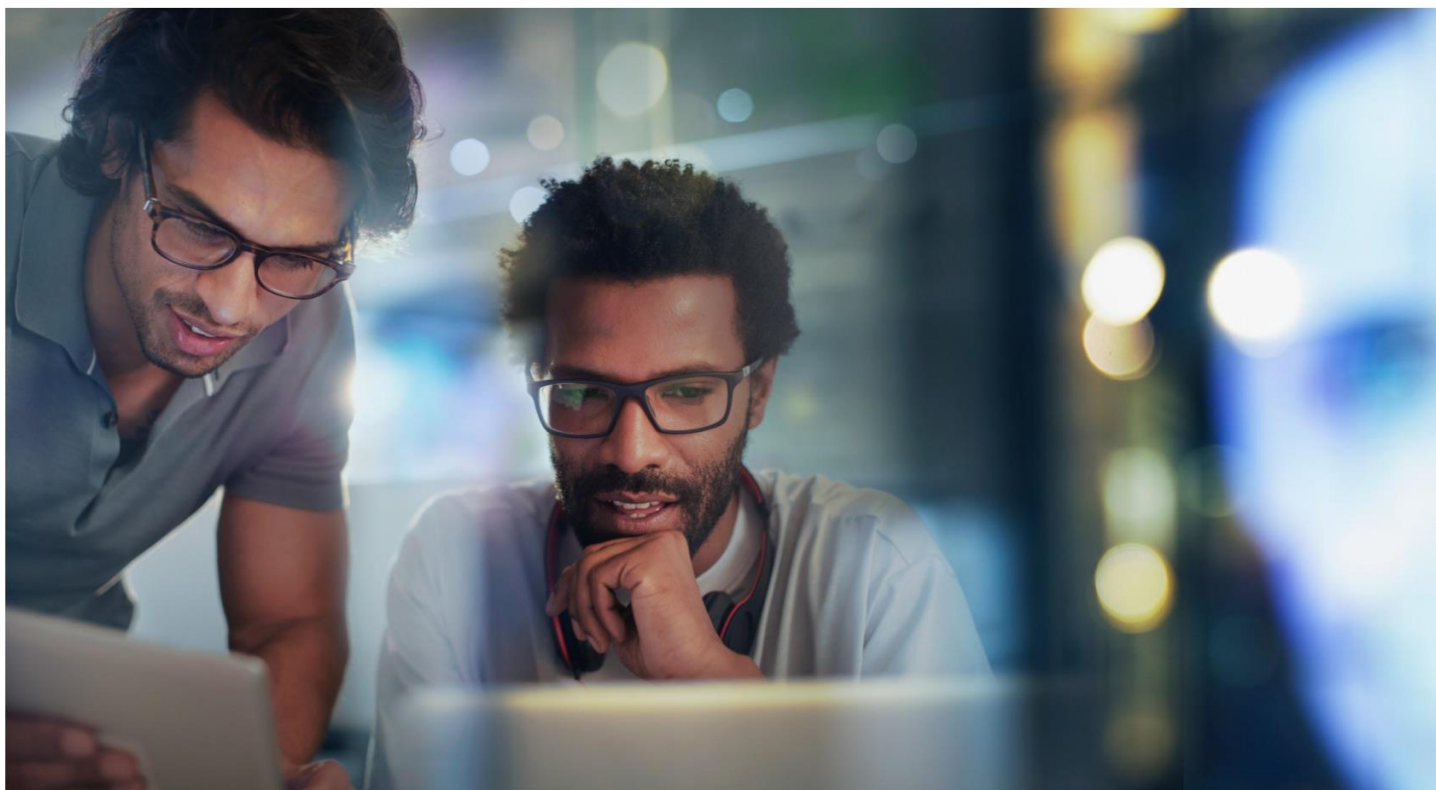


# Compliance programme

Establishing an effective compliance programme is critical to evaluate if control effectiveness is aligned with the PwC ISP Framework, client expectations and regulatory requirements. The compliance programme provides for evaluating control compliance and effectiveness to meet the ISP Framework as well as legal or regulatory and contractual requirements. The internal PwC information security compliance programme should produce transparency on the overall sufficiency and effectiveness of the information security environment.

## ISO 27001

The PwC network information security compliance team has maintained an ISO certification covering their audit programme which is subject to annual audits by independent practitioners.



# Appendix A – Common terms and definitions

Term	Definition
Critical	A classification applied to information, technology, software or physical assets that if disrupted, disabled or significantly impacted for more than four hours would impact on the ability of the business unit and/or member firm to conduct business.
PwC Personnel	Partners, principals, staff, secondees, and third-party labour (including, without limitation, contractors, consultants and temporary employees) of all PwC member firms, including affiliates and subsidiaries.
Endpoint	Computer hardware device that can access information on the PwC network. Computer hardware devices include desktop computers, laptops, smartphones, tablets, thin clients, printers and voice over IP telephony devices.
External connections	Remote users or computers used to connect to the internal PwC network through the use of private network, modem, Internet and other network connections that facilitate internal PwC network activity from a location outside a member firm facility.
Personal data	Any information about a person or from which a person can be identified. Personal data need not be tied to a name and can include public data. If a person cannot be identified or re-identified from the data, the data is not personal data..
Privileged access, Privileged user	Privileged users have higher levels of access than general users. Privileged users are granted access to network devices, systems, applications and/or data from elevated (read-only) up to administrative (read/write) permissions. These permissions may allow access to change or delete data, data structure, user access, access models, application/system configuration and/or application code.
PwC	PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see <a href="https://www.pwc.com/structure">pwc.com/structure</a> for further details.
Security incident	An act or event that violates information security policies, controls, standards or relevant local laws and regulations. Security incidents can be triggered by a single event such as a virus outbreak or network breach. Often, security incidents are a combination of several seemingly innocuous events which if not identified, contained and eradicated in a timely manner, can lead to larger events that pose greater risk to an entire organisation.
Third party	An organisation or person that is not a member of the PwC network.
Critical	A classification applied to information, technology, software or physical assets that if disrupted, disabled or significantly impacted for more than four hours would impact on the ability of the business unit and/or member firm to conduct business.

# Thank you

[pwc.com](https://pwc.com)

© 2023 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.